AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kathryn I. Murray, a Special Agent with Homeland Security Investigations, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic device known as an Apple iPhone 7 Plus (S/N: F2LT35VZHFY2), hereinafter the "SUBJECT DEVICE," further described in Attachment A, for the items described in Attachment B. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

2. Since August of 2004, I have been a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), Allentown, Pennsylvania Office. My duties include the investigation of criminal violations, including violations related to child exploitation and child pornography offenses, such as the production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)) in all forms of media, including digital media.

3. I have participated in the execution of numerous search warrants, a number of which involved child exploitation and/or child pornography offenses. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, among others, and I am authorized by law to request a search warrant.

4. The statements in this affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct) and 18 U.S.C. § 2252(a)(4)(B) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct) are presently located on the SUBJECT DEVICE.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of Title 18 U.S.C. § 2252(a), which prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts to do so.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short

in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. §§ 2256(6), 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing

devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

i. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses may also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. "Mobile application" or "chat application," as used herein, is a specialized program downloaded onto a mobile device, computer, or other digital device that enables users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

m. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, digital, or magnetic form.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. An image can depict the lascivious exhibition of the genitals or pubic area even if the child is clothed, *see United States v. Knox*, 32 F.3d 733 (3d Cir. 1994), *cert. denied*, 513 U.S. 1109 (1995); *United States v. Caillier*, 442 F. App'x 904 (5th Cir. 2011), so long as it is sufficiently sexually suggestive under the factors outlined in *United States v. Dost*, 636 F. Supp. 828 (S.D. Cal. 1986), *aff'd sub nom*, *United States v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *aff'd*, 813 F.2d 1231 (9th Cir. 1987), *cert. denied*, 484 U.S. 856 (1987)

o. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

p. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

7. Based on my training, experience, and research, I know that the SUBJECT DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, and portable

media player, among other capabilities. Further, I know that the SUBJECT DEVICE is a device capable of accessing the Internet.

SUMMARY OF INVESTIGATION

8. On October 5, 2017, Matthew FLYNN pled guilty to a one count of possessing obscene visual representations of the sexual abuse of children, in violation of 18 U.S.C. § 1466A. On February 15, 2022, the Honorable Jeffrey L. Schmehl sentenced FLYNN to time served and twenty years of supervised release. In addition to the standard conditions of supervised release, the terms of FLYNN's supervised release also prohibited him from having access to the Internet, with limited exceptions not relevant here, and prohibited him from possessing Internet-capable devices. Flynn was also prohibited from having any form of contact with minors unless he was supervised by two behavioral healthcare staff members.

9. On May 3, 2023, FLYNN was remanded into custody by Judge Schmehl due to the revocation of his supervised release based on serious physical threats and racial slurs FLYNN repeatedly directed at home healthcare staff. FLYNN was also found in violation of his supervised release based on his unsuccessful discharge from his required sex offender and mental health treatment program.

10. Upon returning FLYNN's personal belongings to his room following his incarceration, home healthcare staff observed the SUBJCET DEVICE, specifically, an Apple iPhone 7 Plus smartphone (S/N F2LT35VZHFY2), in plain view in FLYNN's room and alerted FLYNN's assigned United States Probation Officer ("USPO") from the Eastern District of Pennsylvania Probation Office.

11. Given the terms of FLYNN's supervised release, the USPO seized the SUBJECT DEVICE from FLYNN's residence, located at 102 West Main Street, Elverson, Pennsylvania, and secured the SUBJECT DEVICE consistent with U.S. Probation Office protocols. The USPO subsequently made a request for forensic analysis of the SUBJECT DEVICE.

12. On May 24, 2023, a Supervising U.S. Probation Officer met with FLYNN at the Lehigh County Jail in Allentown, Pennsylvania and secured both written and verbal consent from FLYNN to conduct a forensic analysis of the SUBJECT DEVICE. FLYNN provided the password for the device, and he provided a written statement asserting that the SUBJECT DEVICE belonged to him and that he had obtained the SUBJECT DEVICE from his parents' home on April 15, 2023. FLYNN claimed that the SUBJECT DEVICE did not have Internet access and that he used the SUBJECT DEVICE only to listen to music. He did not make any admissions regarding searching for and/or viewing child pornography on the SUBJECT DEVICE.

13. The SUBJECT DEVICE was forensically analyzed by the U.S. Probation Office. The lock screen of the SUBJECT DEVICE has a June 25, 2017 photograph of FLYNN with a young, unidentified, prepubescent Caucasian male with blonde hair. The home screen of the SUBJECT DEVICE has a January 25, 2015 picture of FLYNN with a different, unidentified, prepubescent Caucasian male.

14. Cellebrite Universal Forensic Extraction Device ("UFED") software was able to obtain a full file extraction as well as an advanced logical extraction, and Cellebrite Physical Analyzer ("Cellebrite") software hashed and verified the content as being accurate.[1] Among other

[1] Based upon my training and experience and information related to me by agents and others involved in the forensic examination of electronic devices, I know that performing a forensic

items, the extraction yielded a total of 155,134 images and 6,738 videos. The dates of the media range from 2015 through May 1, 2023 (2 days prior to FLYNN's detention for violating the conditions of his supervised release), when FLYNN took a photograph of himself at 1:13 p.m. Much of the media content (thousands of images and videos) appear to be child sexual abuse material of prepubescent males engaged in oral and anal sex. There are numerous images and videos depicting adult males engaging in oral and anal sex with prepubescent males as well.

15. Many items appear to have been downloaded and viewed while FLYNN was awaiting sentencing by Judge Schmehl for his 2017 conviction. It is noted that FLYNN's supervised release was initiated on February 15, 2022. At least some of the child pornography on the device appears to have been obtained and accessed after that date. For example, based on the metadata contained in the files, the following two videos appear to have been downloaded and accessed on December 1, 2022 and depict prepubescent boys masturbating:

a. Trim.E3EE5EB0-2DA1-4044-B146-DF6B87E0366A.MOV

b. Trim.451B0FA5-4432-4B6F-BB31-F5279DF5D19.MOV

16. On May 1, 2023, FLYNN created a memo within the SUBJECT DEVICE that says: "Try to contact +18573099169 by Text message to see if he can text message me some CP[2] boys porn videos to me whenever I have a chance to contact him."

17. The extraction also showed that Flynn accessed the following social media sites from the SUBJECT DEVICE, in violation of the terms of his supervised release:

---

analysis of a device will not alter, change, add, or delete any information contained within the device.

[2] I know from my training and experience, that "CP" stands for "child pornography."

a. Google+

b. Facebook

c. Instagram

d. Kik

e. Musically

f. Snapchat

g. Tumblr

18. FLYNN also used the following communication software on the SUBJECT DEVICE, in addition to the native messaging application, in violation of the terms of his supervised release:

a. Microsoft Teams

b. Google Hangouts

c. Skype

19. Additionally, several email accounts were captured in the extraction with at least one being active through May 3, 2023, the date when FLYNN was remanded into custody.

20. I know from my training and experience that the social media and communication applications listed above can be used to communicate via the Internet with other individuals, including by sending written messages, photographs, and videos.

21. Further, during HSI's previous investigation into FLYNN, which led to his 2017 conviction, FLYNN used both the Kik and Musically applications to communicate with minors.

22. On August 28, 2023, HSI seized the SUBJECT DEVICE pursuant to an ongoing investigation and in anticipation of submitting this federal search warrant for the SUBJECT DEVICE.

23. While HSI might already have all necessary authority to examine the SUBJECT DEVICE, I seek this additional warrant out of an abundance of caution to be certain that an examination of the SUBJECT DEVICE will comply with the Fourth Amendment and other applicable laws.

24. The SUBJECT DEVICE is currently in secure storage at HSI Philadelphia. In my training and experience, I know that the SUBJECT DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE first came into the possession of HSI.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

25. As described in Attachment B, this application seeks permission to search for images, videos, and records that might be found on the SUBJECT DEVICE, in whatever form they are found. Thus, the warrant applied for would authorize the seizure and search of the SUBJECT DEVICE pursuant to Rule 41(e)(2)(B).

26. There is probable cause to believe that records will be stored on the SUBJECT DEVICE, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have

been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer or electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain

information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer and electronic storage devices were used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE AND POSSESS CHILD PORNOGRAPHY

28. Based on my education, training, and experience, as well as information obtained from other experience law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce and possess child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including, but not limited to print and digitized/electronic media. Individuals who have a sexual interest in children or images of children often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain this material for many years.

d. Likewise, such individuals often maintain their child pornography images and videos in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are highly valued. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Based on the investigation to date, FLYNN is an individual who has produced and possessed child pornography.

i. Because material depicting minors engaged in sexually explicit conduct was found on all of the electronic devices seized from FLYNN's residence, that the SUBJECT DEVICE is designed to copy, store, or backup data from other devices, that FLYNN has been identified as an individual who produces and collects images and videos depicting children engaged in sexually explicit, and that that the SUBJECT DEVICE was identified as being the property of FLYNN, there is probable cause to believe that evidence outlined in Attachment B will be found on the SUBJECT DEVICE.

CONCLUSION

29. Based upon the information above I respectfully submit that there is probable cause to believe that violations of Title 18 U.S.C. Sections 2252 have been committed and that evidence of those violations is located on the SUBJECT DEVICE. This evidence, listed in Attachment B to

this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses. Therefore, I respectfully request that the attached warrant be issued authorizing the search and seizure of the SUBJECT DEVICE identified in Attachment A, for the items listed in Attachment B.

_/s/ Kathryn I. Murray_____
Kathryn I. Murray
Special Agent
Homeland Security Investigations

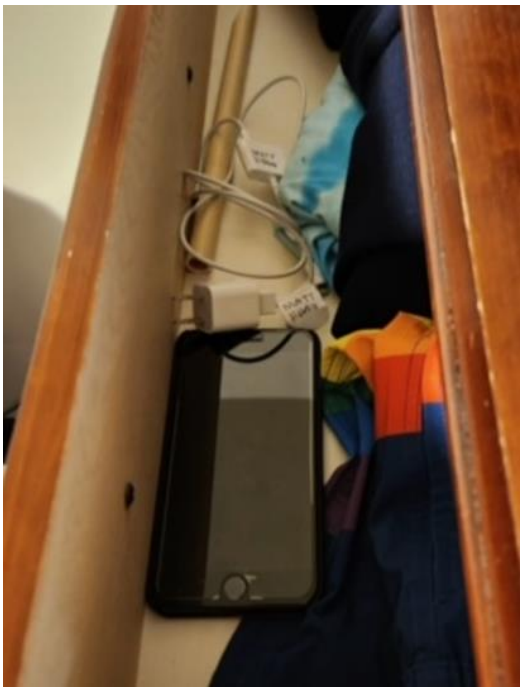
Sworn and subscribed
before me this 26th day
of September, 2023.

/s/ PAMELA A. CARLOS
PAMELA A. CARLOS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF DEVICE TO BE SEARCHED

Black iPhone 7 Plus bearing serial number F2LT35VZHFY2 (pictured below), which is currently located in secure evidence storage at Homeland Security Investigations/SAC Philadelphia Office:



ATTACHMENT B

DEVICE TO BE SEARCHED FOR AND SEIZED

Evidence of violations of Title 18 U.S.C. Section 2252, including the following:

1. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct.

2. All digital records and documents including contact information, text messages, call logs, voicemails, Internet searches, photographs, and any other electronic data.

3. All communications and files with or about potential minors involving sexual topics or in an effort to seduce the minor or efforts to meet a minor.

4. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.

5. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

6. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device.

7. Documents and records regarding the ownership and/or possession of the subject device.

8. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

9. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were

opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer or device at the time any of the items described in paragraph 1-3 were created, sent, received, or viewed. Also, any malware resident on the electronic device.